UNITED STATES DISTRICT COURT

DISTRICT OF OREGON

PORTLAND DIVISION

UNITED STATES OF AMERICA,

Plaintiff,

v.

JOHN HENRY AHRNDT,

Defendant.

Criminal Case No. 3:08-CR-00468-KI

OPINION AND ORDER ON MOTION TO SUPPRESS

S. Amanda Marshall
United States Attorney
District of Oregon
Gregory R. Nyhus
United States Attorney's Office
1000 SW Third Ave., Ste. 600
Portland, OR 97204

Attorneys for Plaintiff

Francesca Freccero
Federal Public Defender's Office
101 SW Main St., Ste 1700
Portland, OR 97204

Attorney for Defendant

KING, Judge:

John Henry Ahrndt moves to suppress evidence and statements obtained as a result of a warrantless search made by a police officer's connection to Ahrndt's personal wireless network and opening one of his shared files. Pending before me is Ahrndt's renewed Motion to Suppress [23, 69]. For the following reasons, I grant the motion and suppress evidence agents discovered on Ahrndt's storage media and the subsequent statements he made to them.

BACKGROUND

I. Procedural History of the Case

Ahrndt was indicted on October 16, 2008 with one count of Transportation of Child Pornography and one count of Possession of Child Pornography.

I denied Ahrndt's motion to suppress on January 28, 2010, and defendant entered a conditional guilty plea to Count 2. The government dismissed Count 1 and I sentenced Ahrndt to the mandatory minimum of 120 months on Count 2. I allowed release pending appeal.

In an unpublished memorandum, the Ninth Circuit reversed and remanded for additional fact finding. United States v. Ahrndt, 475 F. App'x 656, 657 (9th Cir. 2012) [60] (hereinafter, "Ahrndt II"). While awaiting briefing for the second evidentiary hearing, I granted Ahrndt's

motion to withdraw his previous guilty plea and I granted the United States' motion to dismiss Count 1. Accordingly, Possession of Child Pornography is the only remaining charge.

I held a second evidentiary hearing on November 15, 2012, again taking the testimony of Ahrndt's expert witness, Robert Young. The government declined to present additional evidence.

II. Background Facts

After the second evidentiary hearing, and considering the evidence adduced at the first evidentiary hearing, I find as follows:

On February 21, 2007, a woman referred to as JH was using her personal computer at her home in Aloha, Oregon. She was connected to the internet via her own wireless network, but, when her wireless network malfunctioned, her computer automatically picked up another nearby wireless network called "Belkin54G." Belkin54G refers to a wireless router, made by the company Belkin, that broadcasts a wireless signal in a roughly 400 foot radius. Its default setting has no security. At the second evidentiary hearing, defense expert Robert Young testified that JH's laptop would not have automatically connected to Belkin54G the first time she lost her own wireless signal. Instead, her computer would have sent a signal to search for wireless routers within range of her computer and the names of available wireless routers would have appeared in a list on her computer. JH would have clicked on Belkin54G to prompt her computer to connect to that wireless router. If the wireless router was secured, she would have had to enter a password to connect to the wireless router. Because the Belkin54G was not secured, JH connected without entering a password. From that time forward, her computer remembered the available connection and she did not have to select Belkin54G again when her own wireless

signal failed. Nevertheless, even after that first time, in order to connect to Belkin54G, JH's computer needed to send a signal into Ahrndt's computer and the router's processor to use the wireless network.

A Belkin54G router comes with an installation CD containing a manual instructing on the "importance of security measures," according to the testimony of Agent Tony Onstad at the first evidentiary hearing. Tr. of Hr'g on Mot. to Suppress 31: 24-32:1 (Jan. 7, 2010) [59] (hereinafter, "First Hr'g Tr."). There is no evidence Ahrndt had read or received this manual. The government did not introduce the manual itself.

After JH connected to the internet via the Belkin54G wireless network, JH opened her iTunes software to listen to music. The iTunes software is designed to organize and play audio, video, and image files. The iTunes software also allows users to browse music and video that is stored in the iTunes libraries of other computers on the same network, if those libraries are enabled to "share." In addition, accepting Young's testimony, iTunes software installed on one computer ("computer 2") integrates with LimeWire installed on another computer ("computer 1") so that when the two computers are on the same network iTunes will display media on computer 2 available through LimeWire on computer 1. In this case, when JH opened her iTunes, she noticed another user's library–called "Dad's LimeWire Tunes"–was available for sharing. Young also testified that the name "Dad's LimeWire Tunes" was an automatically generated folder name.

JH opened Dad's Limewire Tunes and observed files with names that prompted her to call the Washington County Sheriff's Office a little before 10:45 p.m. The transcript reflects the following interaction:

> JH: Ok, Um, I just um was looking at my ITunes um and I, you can share music with people that are I guess in your area and I was just um sharing some music with this I guess it's a neighbor of mine, I have no way of knowing where they are or whatever but it's a whole bunch of um underage child pornography. I just wanted somebody to know about that.

Def's. Ex. 103 (First Hr'g).

She gave her name, address and phone number. When asked, "And how long ago did you get, receive that?" she answered,

> JH: Um, Its up there now. I just turned on my computer and turned on my Itunes and just saw that I was sharing music so I just checked it and um I just saw it. I mean I didn't open any of the stuff but the names are all stuff about 11 year old girls and 9 year olds you know, just stuff that I don't it sounds inappropriate.

Id.

Washington County Deputy John McCullough arrived a little less than an hour later. Deputy McCullough noted in his police report that JH showed him a "play list of approximately 25 picture and video files. The files had pornographic titles that indicated the images were of underage children." Def's. Ex. 104, at 4 (First Hr'g). At first, they were not able to open the files or identify an owner. Deputy McCullough called his sergeant. Deputy McCullough testified at the first suppression hearing that he called his sergeant for two reasons: to advise him what he had learned and to "determine if it would be appropriate or not for me to look further into those files and try to determine what was enclosed within them." First Hr'g Tr. 8:8-12. After speaking with his supervisor, Deputy McCullough concluded it would be acceptable to investigate further and he requested that JH attempt to open one of the files.[1] The two saw a

[1]In his report, Deputy McCullough wrote that while he was talking with his supervisor, JH informed Deputy McCullough that she could open one of the files. The government concedes, (continued...)

sexually explicit image of a boy masturbating. JH's computer then lost the signal and she was unable to open any other files.

JH informed Deputy McCullough that the Belkin54G showed as an available wireless network on her computer when she moved in. At that time, only one resident lived in her new development. She then pointed out an older house nearby, about 150 feet away, which was the only other home she knew was occupied when she moved in. Deputy McCullough subsequently ran the license plates of a car in the driveway of that house and learned that defendant John Henry Ahrndt, a convicted sex offender, lived there. Fredrick Harmon, a friend and tenant of defendant, also lived at the residence.

Two days later, on February 23, 2007, Washington County Sheriff's Office Detective Ray Marcom and Department of Homeland Security, U.S. Immigration and Customs Enforcement, Senior Special Agent James Cole interviewed JH further about the incident. JH repeated to Marcom and Cole much of what she had told Deputy McCullough. She also remembered one file name specifically: "11-yr old masturbating." She generally remembered words such as "tiny," "fuck," and "cunt," in conjunction with acronyms indicating age like "5yoa" and "8yoa." Def's. Ex. A, at AHRNDT R004 [25].

Agent Cole also spoke with Deputy McCullough, who could not remember specific filenames. He nevertheless reported observing that some of the age acronyms in the files, like "5yoa," were followed by the words "getting raped" and "being raped." Id.

On April 2, 2007, Agent Cole applied to United States Magistrate Judge Dennis Hubel for

---

[1](...continued)
however, that JH was acting as an agent of the government when she opened the image. Gov't. Second Resp. 34 [72].

a search warrant to access the Belkin54G wireless network for the purpose of determining the internet protocol ("IP") address associated with the router. An IP address would allow investigators to find out from an internet service provider who owned the Belkin54G wireless network. Judge Hubel granted the warrant the same day. On April 7, 2007, Agent Cole drove near the house, accessed the Belkin54G network, and determined the network's IP address. Through the American Registry for Internet Numbers, Agent Cole learned that the IP address belonged to Comcast. He served a summons on Comcast and learned that Ahrndt was the Comcast subscriber for the IP address in question.

On April 17, 2007, Agent Cole obtained a second search warrant from Judge Hubel allowing a search of the home for wireless routers, computers, and any files or storage media that could contain images of child pornography. The next morning officers searched defendant's home and seized one tower computer, a Belkin wireless router, various hard drives, numerous disc media and flash media.

Agents interviewed Ahrndt when they executed the second search warrant. They told him he was not under arrest and that he was free to leave at any time. Ahrndt stayed and agreed to speak to the agents. He admitted to downloading child pornography as recently as eight months previously using the peer-to-peer file-sharing software LimeWire, but that he had deleted any images he downloaded from that time. Def's. Ex. A, at AHRNDT R0027 [25]. He also told agents that he had deleted all the images he had previously obtained, but that they would find child pornography images if they were capable of recovering deleted images. Specifically, he told the agents they would find deleted images on his external hard drives, which he had converted from hard drives of his old computers. He denied, however, that there was any child

pornography on his current computer, which he had obtained from a member of his church in January 2007. Ahrndt also told agents that no one else used his computer, but that Mr. Harmon, his friend and tenant, used the wireless network.

A subsequent computer forensic examination of the equipment found 20 images, 17 of which depicted children engaged in sexually explicit conduct. The first three images were advertising pages located in an "orphan" file, meaning its parent file had been deleted. The next four images were located in a Google Hello "scache," indicating the images had been sent or transmitted. Image 8 was a .mpg movie that had been viewed in Windows Explorer or by using a My Computer thumbnail or filmstrip view. Image 9 was a deleted file recovered from Ahrndt's computer. The last ten images were deleted files recovered from the USB flash drive. Agent Cole's forensic report did not mention LimeWire, any share folder created by LimeWire, or iTunes.

Ahrndt's expert Young testified at the second evidentiary hearing that when LimeWire is installed, the user has the option of directing LimeWire to start automatically when the user logs into his computer allowing the program to start faster. The default then becomes an automatic start for LimeWire when the user logs in to his computer, allowing LimeWire to run the entire time the user is on his computer. Young also explained LimeWire's default setting is to share content "on the Local Area Network and make it accessible for Itunes and other Digital Audio Access Protocol 'DAAP' enabled Players." Def's. Ex. 101 (Second Hr'g).

There is no evidence Ahrndt was using iTunes or deliberately sharing files. There is evidence Ahrndt had used LimeWire to download child pornography eight months before, but no evidence he had set his program to share files over the internet.

Ahrndt brought a motion to suppress all evidence seized after Deputy McCullough's initial access of Ahrndt's files through JH's computer, on the theory that without Deputy McCullough's actions the first and second warrants would not have issued.

LEGAL STANDARDS

The Fourth Amendment to the Constitution establishes the rights of American citizens to be free from unreasonable searches and seizures by the government. U.S. Const. Amend. 4. A warrantless search is *per se* unreasonable unless it is justified by an exception to the general rule. Horton v. California, 496 U.S. 128, 133 (1990).

Private party conduct does not implicate the Fourth Amendment; only activity by government agents raises Fourth Amendment concerns. United States v. Young, 153 F.3d 1079, 1080 (9th Cir. 1998) (per curiam).

In order to invoke the Fourth Amendment, a defendant must show that his Fourth Amendment rights have been implicated; that is, he must show a "search" occurred at all before requiring the government to prove an exception to the warrant requirement. The Ninth Circuit spelled out the applicable standard in its opinion in this case as follows:

> A search occurs when the government violates an individual's reasonable expectation of privacy. See United States v. Jacobsen, 466 U.S. 109, 113 (1984). "An individual has a reasonable expectation of privacy if he can demonstrate a subjective expectation that his activities would be private, and he [can] show that his expectation was one that society is prepared to recognize as reasonable." United States v. Heckenkamp, 482 F.3d 1142, 1146 (9th Cir. 2007) (internal quotation marks omitted) (alteration in original). A search also occurs whenever "the Government obtain information by physically intruding on a constitutionally protected area." United States v. Jones, 132 S. Ct. 945, 950 n. 3 (2012).

Ahrndt II, 475 F. App'x at 657.[2]

DISCUSSION

I. The Private Search

"The Fourth Amendment limits searches conducted by the government, not by a private party, unless the private party acts as an 'instrument or agent' of the government." Young, 153 F.3d at 1080; United States v. Black, 767 F.2d 1334, 1339 (9th Cir. 1985) ("A wrongful search or seizure conducted by a private person does not violate the Fourth Amendment," describing personal assistant's disclosure of her employer's documents when she was not authorized to disclose them). Here, JH discovered the list of images contained in Ahrndt's LimeWire folder while using her own iTunes program and Ahrndt's unsecured wireless network.

Although I have already concluded JH did nothing illegal, United States v. Ahrndt, Criminal No. 3:08-468-KI , 2010 WL 373994, at * 8 (D. Or. Jan. 28, 2010) [45] (hereinafter, Ahrndt I"), even if she had courts have declined to suppress evidence even when it was obtained by an individual who had no authorization to access the defendant's computer. See United States v. Kline, 112 F. App'x 562, 564 (9th Cir. 2004) (private individual searched defendant's computer using a "Trojan Horse" computer virus to illegally download files from the infected computer); see also United States v. Jarrett, 338 F.3d 339 (4th Cir. 2003) (child pornography recovered via hacker's actions on computer was not subject to suppression); United States v. Steiger, 318 F.3d 1039 (11th Cir. 2003) (individual's access to a computer by hacking not subject

[2]Because the search here is a remote search of transmitted data, I reject Ahrndt's argument that this was a presumptively unreasonable search inside his home. In addition, although Ahrndt made the same argument to the Ninth Circuit, the Circuit set out the test I quoted above for determining whether a search occurred. Appellant Reply Br. 2.

to the Fourth Amendment); see also Walter v. United States, 447 U.S. 649, 656 (1980) ("[A] wrongful search or seizure conducted by a private party does not violate the Fourth Amendment and . . . such private wrongdoing does not deprive the government of the right to use evidence that it has acquired lawfully.") (plurality opinion). Accordingly, JH's report of the filenames she viewed is not subject to suppression.

Although there is a question whether Deputy McCullough could reenact JH's search by asking her to connect to Ahrndt's unsecured wireless network, open her iTunes, and open the folder called "Dad's LimeWire Tunes," as a practical matter Deputy McCullough's duplication of JH's efforts revealed nothing new that would affect my analysis below. I do note that in my view, under Jacobsen, Deputy McCullough could properly view data on JH's computer when JH had previously performed the search. As the Supreme Court explained in Jacobsen, "Once frustration of the original expectation of privacy occurs, the Fourth Amendment does not prohibit governmental use of the now-nonprivate information . . . . The Fourth Amendment is implicated only if the authorities use information with respect to which the expectation of privacy has not already been frustrated." 466 U.S. at 117 (reliance on Walters, 447 US. 649 in which private party opened mis-delivered package). I am not persuaded by Ahrndt's citation to United States v. Young, 573 F.3d 711 (9th Cir. 2009), in which the court declined to expand Jacobsen to a search of a hotel room, deemed equivalent to a private residence; the invasive action at issue here is a remote search of computer data transmitted on an unsecured wireless network.

I agree with the government, then, that Deputy McCullough saw data on a network that the private party had previously searched. As a result, Deputy McCullough's view of the list of titles in Dad's LimeWire Tunes did not violate Ahrndt's Fourth Amendment rights. There would

be no different outcome, however, even if I am wrong about that conclusion and Deputy McCullough's recollections of the filenames he saw must be excised from the affidavit.

I next consider whether Deputy McCullough's additional step of clicking the image, an action which exceeded the private search, violated Ahrndt's Fourth Amendment rights.

II. Whether Opening of the Image Violated Ahrndt's Fourth Amendment Rights

Deputy McCullough directed JH to open an image. She had not previously opened any of the images. The opened image was no longer within the purview of the private search. I liken the unopened image to the unviewed films at issue in Walter; in that case, the private party had not viewed the suspect films and, prior to the agents' action of watching the films, "one could only draw inferences about what was on the films. The projection of the films was a significant expansion of the search that had been conducted previously by a private party and therefore must be characterized as a separate search." 447 U.S. at 657. I, furthermore, reject the government's argument that the contents were already exposed. Id. at 659 n.13 ("A partial invasion of privacy cannot automatically justify a total invasion.").

The next question is whether Deputy McCullough's action of clicking on the image violated Ahrndt's Fourth Amendment rights. In order to assess Ahrndt's Fourth Amendment rights, I must evaluate whether any subjective expectation of privacy was objectively reasonable. As the Ninth Circuit pointed out, my previous opinion incorrectly framed the issue as whether it is reasonable to have an expectation of privacy in the contents of a *shared iTunes library* on a personal computer connected to an unsecured home wireless network. In fact, the issue is whether it is reasonable to have an expectation of privacy in the contents of a LimeWire file,

when there is no evidence of intentional sharing over the wireless network or the internet, on a personal computer connected to an unsecured home wireless network.

As an initial matter, I conclude Ahrndt's reasonable expectation of privacy in the contents of his computer was not eliminated when he attached it to his unsecured wireless network router. Indeed, as the court stated in Heckenkamp, "the mere act of accessing a network does not in itself extinguish privacy expectations, nor does the fact that others may have occasional access to the computer." 482 F.3d at 1146-47 (citing Leventhal v. Knapek, 266 F.3d 64, 74 (2d Cir. 2001)).

It is true the Heckenkamp court went on to comment that privacy expectations may be reduced if the user is advised the information may not remain confidential or communications may be monitored. Here, with respect to Ahrndt's Belkin54G wireless router, the default setting was unsecured. The quick set-up manual did not discuss security measures that could or should be taken. Although defense counsel stipulated the router came with a manual, and the government's expert testified the manual included detailed instructions on setting up wireless security, the only evidence in the record is that the manual warned of the importance of security. I underscore there is no evidence the manual warned Ahrndt that the *content* of files may be accessible to others, as opposed to just internet access, by failing to secure his router. Accordingly, although Ahrndt's failure to secure his network suggests a lesser subjective expectation of privacy, I could not say he lost all expectation of privacy in the contents of files on his personal computer.

The situation is, of course, a bit more complicated; the evidence suggests the content became available to JH by virtue of the fact that the materials were contained in a LimeWire folder. Nevertheless, although the folder appearing in JH's iTunes directory was called "Dad's

LimeWire Tunes," there is no evidence Ahrndt was sharing files on the peer-to-peer network, and the government concedes there is no evidence the image in Dad's LimeWire Tunes library that JH and Deputy McCullough opened was accessible over the internet by LimeWire users at the time JH and Deputy McCullough accessed the files, or at any time prior. Accordingly, I could not say Ahnrdt had no right to privacy in those files just by virtue of his use of LimeWire to download images. Cf. United States v. Ganoe, 538 F.3d 1117, 1127 (9th Cir. 2008) (denying defendant's motion to suppress evidence on the ground the defendant had installed file sharing software on his computer and was "explicitly warned before completing the installation that the folder into which files are downloaded would be shared with other users in the peer-to-peer network").

Instead, accepting Young's testimony, the evidence suggests LimeWire was likely configured to run whenever Ahrndt turned his computer on. The evidence also suggests the program was set to its default mode of sharing content on Ahrndt's "Local Area Network" making that content "accessible for Itunes and other Digital Audio Access Protocol (DAAP) enabled Players." Def's. Ex. 101 (Second Hr'g). As a technical matter, with respect to the content itself, Young could not say whether iTunes was asking, "Anything to share?" or LimeWire was advertising that it had content to share. Regardless, in order to preclude LimeWire from sharing with iTunes on his network, Ahrndt would have had to seek out and uncheck the sharing option, or choose to require a password for those wishing to access the contents of his LimeWire file. Accordingly, in response to the Ninth Circuit's query, there is no evidence Ahrndt "intentionally" enabled sharing of his files over his wireless network. Ahrndt II, 475 F. App'x at 658. Rather, as Young explained, JH's iTunes software could detect files that

were shared, by default, by Ahrndt's LimeWire program. The government offered no evidence to dispute Young's testimony.

The government suggests Ahrndt had no objective expectation of privacy as a result of the automated computer process that shared his folder, but I find the government's supporting case citations inapt. The government first quotes extensively from the *dissent*'s opinion in Lavan v. City of Los Angeles, 693 F.3d 1022, 1038-39 (9th Cir. 2012). The only other Ninth Circuit case referenced by the government is United States v. Borowy, 595 F.3d 1045 (9th Cir. 2010) (per curiam), but in that case the agent found the images via the internet by browsing the shared content stored in defendant's LimeWire file. Although the defendant had attempted to prevent LimeWire from sharing his files over the internet, his "subjective intention . . . did not create an objectively reasonable expectation of privacy in the face of such *widespread public access*." 595 F.3d at 1048 (emphasis added); compare United States v. Sawyer, 786 F. Supp. 2d 1352, 1356 (N. D. Ohio 2011) (somewhat more reasonable expectation of privacy in content shared with "friends" over an open program, but no control over manner in which "friends" used their access, so no objective expectation of privacy). Here, the evidence suggests Ahrndt unknowingly, and by default of the program, shared the content stored in his LimeWire folder over his home wireless network. This was not the widespread public access found to have undermined Borowy's expectation of privacy.

Finally, both United States v. Procopio, 88 F.3d 21 (1st Cir. 1996), and United States v. O'Bryant, 775 F.2d 1528, 1534 (11th Cir. 1985), involved unintended disclosures of private documents as a result of third party actions, thereby destroying any objective expectation of privacy. Neither case is persuasive. In Procopio, a private party stole a safe, leaving it open in a

park with papers inside and outside the safe, but the officer did not exceed the scope of the private search as Deputy McCullough did here. In O'Bryant, an officer found a stolen briefcase next to a dumpster and the court explained that abandoned valuable property may be inspected to determine the identity of the owner and to inventory the contents. Finally, both of these cases arose outside the Ninth Circuit.

In short, the government does not dispute a person has a reasonable expectation of privacy in the files on his home personal computer. There is no evidence Ahrndt was using iTunes software or any other program to deliberately share files. The evidence is that he had media-enabled files that JH was able to view using her own iTunes program because Ahrndt's files made themselves available, by default, through JH's iTunes. There is no evidence Ahrndt intentionally enabled sharing of his files over his wireless network, and there is no evidence he knew or should have known that others could access his files by connecting to his wireless network. Deputy McCullough's action of clicking on the image in JH's iTunes directory to open the image violated Ahrndt's Fourth Amendment rights. His description of the image, and any related tainted evidence, must be stricken from Agent Cole's affidavit.

III. Single Purpose Container

The government justifies Deputy McCullough's additional click under the "single-purpose container" exception to the warrant requirement. Specifically,

> [n]ot all containers and packages found by police during the course of a search will deserve the full protection of the Fourth Amendment. Thus, some containers (for example a kit of burglar tools or a gun case) by their very nature cannot support any reasonable expectation of privacy because their contents can be inferred from their outward appearance.

United States v. Gust, 405 F.3d 797, 800 (9th Cir. 2005) (quoting Arkansas v. Sanders, 442 U.S. 753, 764 n.13 (1979)). Ultimately, "to fall within the [single-purpose container] exception of [Sanders] a container must so clearly announce its contents, whether by its distinctive configuration, its transparency, or otherwise, that its contents are obvious to an observer." Id. at 801. This evaluation is made "from the objective viewpoint of a layperson." Id. According to the government, the file names alone announced their content. It relies on the district court's decision in Borowy, which concluded, "Here, the filenames are explicit enough that the container is such that its contents may be said to be in plain view. Therefore, [the agent's] viewing of the files' content did not require a warrant." 577 F. Supp. 2d 1133 (D. Nev. 2008), aff'd, 595 F.3d 1045 (9th Cir. 2010) (internal quotation marks and citation omitted).

The Ninth Circuit did not comment on the single purpose use exception in affirming the district court opinion in Borowy, 595 F.3d 1045 (upholding decision; no search occurred because defendant had used peer-to-peer software to share images). Absent more compelling authority, I do not accept the government's invocation of the single purpose container exception particularly when I have relied on the opposite argument made in other cases. See United States v. Kowalczyk, Criminal No. 3:08-95-KI, 2012 WL 3201975, at *24, (D. Or. Aug. 3, 2012) (accepting government's argument that, in executing a warrant, an investigator acted appropriately in opening images of child pornography while looking for identity theft and fraud because file names may be inaccurate and can be changed); see also United States v. Giberson, 527 F.3d 882, 889 (9th Cir. 2008) ("computer records are extremely susceptible to tampering, hiding, or destruction").

IV. Whether the Affidavit Contains Probable Cause After Excising the Opened Image

The government contends that even if Deputy McCullough had not asked JH to open a single file, their observations of the file names displayed openly in JH's iTunes library were sufficient to establish the existence of probable child pornography sufficient to support a warrant to search.

Probable cause exists when there is a "fair probability" of "finding evidence considering the type of crime, the nature of the items sought, the suspect's opportunity for concealment and normal inferences about where a criminal might hide stolen property," or the fruits of his crime. United States v. Parks, 285 F.3d 1133, 1142 (9th Cir. 2002).

Without JH or Deputy McCullough's description of the single image they viewed, the magistrate would have only the following statements made by Agent Cole in his affidavit:

–"JH noted that approximately 25 to 30 of the file names had file names indicating that the file may be child pornography." Def's. Ex. 106, Cole Aff. ¶ 10 (First Hr'g).

–"Deputy McCullough, duplicating what JH had already done, viewed the library list of Dad's Limewire Tunes and observed approximately 25 pictures and video files which had pornographic titles that indicated the files were of underage children." Id.

–When interviewed later, JH "could not specifically recall any other file names [other than the one she had opened]." She remembered that the file names included ages such as "5 yoa, . . . 8 yoa and 9 yoa. JH stated that none of the files had ages higher than 11 years old. JH also noted the words: "Tiny," "fuck," "sick" and "cunt" in the file names. JH believed that based on the filenames she observed that the filenames contained child pornography which is the reason that JH contacted law enforcement." Id. at ¶ 12.

–Deputy McCullough also could not remember specific filenames. He remembered seeing 25 filenames "which purported by their filenames to be files related to the sexual abuse of children." Id. at ¶ 15. He remembered the filenames "contained what appeared to be children's ages including 8 yoa, 9 yoa, 10 yoa and 11 yoa. Deputy McCullough stated that the filenames described sexual activity after the age such as 'being raped' and 'getting raped.' Deputy McCullough believed based on the filenames that the files depicted child pornography." Id.[3]

The government concedes file names are not always definitive as to their contents, but argues the names viewed by JH and Deputy McCullough were highly indicative of child pornography. It cites two cases in support of its theory. The first, United States v. Miknevich, upheld a warrant affidavit based on a single file name, a confirmation that a different officer later viewed the contents, and a computerized file analysis. According to the court, "[t]he unmistakable inference which arises from the file name . . . is that its contents include material pertaining to the sexual exploitation of children" and because a computerized file analysis indicated the contents may have included child pornography. 638 F.3d 178, 185 (3rd Cir. 2011). The government concedes there was no computerized file analysis here, but the magistrate had multiple file names with similar titles, suggesting the files were what they said they were. The other case the government cites, United States v. Battershell, relied on a girlfriend's complaint that the computer contained photos of "kids having sex" and law enforcement officers' brief descriptions of two photographs they had viewed: a "young female (8-10 YOA)" and "another

[3]I do not accept Ahrndt's speculation that JH and Deputy McCullough's recollections of the filenames were tainted by their view of the single image, requiring the excision of paragraphs 11, 12 and 15 in their entirety. Other than JH's memory of the single file name, which matched the image she viewed, there is no evidence of taint and none is obviously apparent.

young female having sexual intercourse." 457 F.3d 1048, 1053 (9th Cir. 2006). This was enough for probable cause. The government argues that, here, seeing the actual image is an added benefit, but suggests probable cause may be satisfied where 25 to 30 files describe sexual acts found in the file sharing software LimeWire.

Ahrndt concedes a magistrate may have authorized the first search warrant to obtain Ahrndt's IP address based on JH's and Deputy McCullough's general assertions. He argues, however, lacking specific titles and the description of an image, a magistrate would never have authorized police to invade Ahrndt's home and search his personal computer.

I agree with Ahrndt. As an initial matter, the Ninth Circuit has described several acceptable ways for an affiant to show the existence of contraband images. The "ideal course" is to provide copies of the alleged pornographic photographs for the magistrate to view, but failing to include such pictures is not "fatal to the warrant[.]" United States v. Smith, 795 F.2d 841, 847 (9th Cir. 1986). Alternatively, a magistrate may rely on an experienced officer's "factual descriptions of an image." Battershell, 457 F.3d at 1053 (officer described in his police report the images he had personally viewed and the report was appended to forensic investigator's affidavit);[4] New York v. P.J. Video, Inc., 475 U.S. 868, 874 n.5 (1986) ("reasonably specific affidavit describing the content of a film generally provides an adequate basis for the magistrate to determine whether there is probable cause to believe that the film is obscene, and whether a warrant authorizing the seizure of the film should issue"). Finally, absent any description of the

[4]In that case, for example, the government conceded a description of "a young female (8-10 YOA) naked in a bathtub" was "insufficient to establish probable cause that the photograph lasciviously exhibited the genitals or pubic area" of the minor, one of the statutory definitions for "sexually explicit conduct." Battershell, 457 F.3d at 1051.

images, a magistrate may rely on an experienced affiant's representation that the photographs he viewed meet the statute's criteria. Smith, 795 F.2d at 848 (magistrate could rely on statement of "experienced postal inspector that the photos depicted 'sexually explicit conduct' within the statute").

The government has not offered any authority where a partial recollection of file names provided sufficient probable cause. The cases cited by the government had more than a description of file names. Miknevich had the "digital fingerprint" supporting the assertion that the image was child pornography. 638 F.3d at 185. Battershell had the statement from a witness that she had seen the images on her boyfriend's computer and described them as "kids having sex." 457 F.3d at 1052. Although I recognize probable cause means a fair probability and "not certainty or even a preponderance of the evidence," given the dearth of case authority I am loathe to find probable cause here absent a view of one image. United States v. Gourde, 440 F.3d 1065, 1069 (9th Cir. 2006) (en banc). Ahrndt suggests instead, and I agree, the deputy should have obtained a warrant to open one of the images. The partial recollections and characterizations of the file names JH and Deputy McCullough saw were too general to support the issuance of a warrant to enter Ahrndt's home and seize his computer and related equipment.

V. Whether the Deputy's Actions were Reasonable, Making Suppression Unwarranted

The government argues Deputy McCullough had no idea the files came from somewhere entitled to Fourth Amendment protection, making suppression unwarranted. The government's argument goes like this: the content was viewed by JH and the deputy on JH's computer, using her network connection, in her residence, using her iTunes program with her permission, and the network on which they viewed the content provided no indication as to the source, or that the

source was one that was of a type that would receive Fourth Amendment protections. Indeed, the name that appeared in JH's iTunes playlist did not indicate a privacy interest or ownership interest (not like "Dad's Medical Records" or "Dad's Tax Records"). Instead, according to the government, the name invited inspection–Dad's Limewire Tunes. JH did not have to seek out Ahnrdt's network; it broadcast its signal and "essentially invited association[.]" Gov't. Second Resp. 10 [72]. The government argues it was not known to the officers that the wireless signal came from another home until the officers got the address two months later from Comcast.

As an initial matter, I reject the government's recitation of the facts. The facts, as adduced at the evidentiary hearing and as reflected in Deputy McCullough's reports, are that JH knew the unsecured wireless signal was resonating from a place in her neighborhood. There is no description of any public place in her neighborhood from which the signal could be emanating. Rather, she and Deputy McCullough identified two places from which the signal could be emanating, both of which were residences. Contrary to the government's assertion, this evidence indicates Deputy McCullough more than likely knew he was directing JH to open a file on a computer in a private neighbor's residence. His testimony confirms he called his supervisor for guidance, also suggesting he knew he needed to be cautious in proceeding.

The government relies on Herring v. United States, 555 U.S. 135 (2009), United States v. Leon, 468 U.S. 897, 906 (1984), and Illinois v. Krull, 480 U.S. 340, 347 (1987), for the proposition that where there is no police misconduct to deter, suppressing the evidence is improper. It argues Deputy McCullough did not evince any deliberate, reckless, or grossly negligent disregard for Ahrndt's Fourth Amendment rights. All of what the government says may be true, but "[t]he good faith exception does not apply where a search warrant is issued on

the basis of evidence obtained as the result of an illegal search." United States v. Wanless, 882 F.2d 1459, 1466 (9th Cir. 1989); United States v. Song Ja Cha, 597 F.3d 995 (9th Cir. 2010) (Ninth Circuit cases holding that the good faith exception does not apply to mistakes of law are still good law after Herring).

I decline to apply the good faith exception to save the warrant here.

VI. Supreme Court Case United States v. Jones

The Ninth Circuit asked me to consider whether the analysis in United States v. Jones, 132 S. Ct. 945 (2012) directed suppression. Since I find suppression is warranted under the framework set forth above, I need not address this issue.

CONCLUSION

For the foregoing reasons, Ahrndt's Motion to Suppress evidence obtained from his storage media and the statements he made to the agents is GRANTED.

IT IS SO ORDERED.

DATED this 17th day of January, 2013.

/s/ Garr M. King
Garr M. King
United States District Judge